UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/693,378	10/23/2003	Chris D. Hyser	200205369-1	1637

22879 7590 07/29/2008

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
ALMEIDA, DEVIN E	

ART UNIT	PAPER NUMBER
2132	

NOTIFICATION DATE	DELIVERY MODE
07/29/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
mkraft@hp.com
ipa.mail@hp.com

Office Action Summary	Application No.	Applicant(s)	
	10/693,378	HYSER, CHRIS D.	
	Examiner	Art Unit	
	DEVIN ALMEIDA	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 April 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5 and 15-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5 and 15-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This action is in response to the papers filed 4/3/2008.

Response to Traverse of Restriction Requirement

Applicant's arguments with respect to the traverse of the restriction requirement have been fully considered but they are not persuasive. In Subcombination I claims 1-5 and 15-18 are directed to a method of generating an authenticable and verifiable image by adding to the module image a size and location block, an authentication block including a cryptographically protected module-specific public key and a clear-text version of the module-specific public key and a verification block that includes a digital signature. In Subcombination II Claims 6-14 have separate utility such as authenticating and verifying an authenticable and verifiable image by comparing the cryptographically protected data with the module-specific public key to authenticate the authenticable and verifiable module and comparing a value calculate from the image including a size and location block included with the authenticable and verification block within the authenticable and verifiable image to verify the authenticable and verifiable module. Subcombination II in not the only way to authenticate and verify the module image of Subcombination I. Another way to authenticate and verify the verify the authenticable image of subcombination I is to have the cryptographically protected module-specific public key encrypted with a private key of a trusted authority is added to the digital image. That way when it is decrypted with the public key of the trusted authority you know the public key is valid public key for that sender. Then the digital signature that was added to the module image can be verified using the module-specific public key to

verify the digital signature that was created by encrypting the hash value of the module image with the sender's private key produces the digital signature. If the digital signature match it is know that the module image has not been altered. This different method of verifying an authenticable and verifiable image also lets the receiver know who the sender of the module image is and that the sender did send the module image and that the module image has not been altered.

Response to Arguments

Applicant's arguments with respect to the word "module" have been fully considered but they are not persuasive. According to the specification the module image can be a software image or a firmware image. Colligan teaches a software image (see abstract) which clearly meets the limitations of the claims.

Applicant's arguments with respect to "adding to the module image a size and location block" have been fully considered but they are not persuasive. In Colligan figure 4 and column 9 lines 14-38 it clearly teaches adding a header file to the image that includes the size and location. The header file is created for the restoration image on the hard drive that includes the size and location and then the factory downloaded image are copied, in compressed form, to the restoration image on the HDD.

Applicant's arguments with respect to "adding to the module image an authentication block including a cryptographically protected module-specific public key and a clear-text version of the module-specific public key to produce an authenticable image" have been fully considered but they are not persuasive. Crumly teaches in paragraph 0025 that a public key is encrypted with the private key of a trusted authority

is added to the digital image. Crumly teaches in paragraph 0036 along with the encrypted image, the sender may include a digital signature that relates to the size and content of the digital image. This digital signature may be a hash value produced from the digital image, either before or after encryption, using a one-way hashing function, such as a digital signature algorithm. Encryption of the hash value with the sender's private key produces the digital signature. **In this case, the sender also may include the sender's public key, allowing the recipient to verify the digital signature.** Including both the public key encrypted with the private key of a trusted authority and the public key in the clear allows the receiver to verify the public key using the digital certificate of the public key and use that public key to verify the image. So that the receive may verify that the decoded digital image has not been altered and was sent by a holder of the sender's private key.

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, it would have been obvious to have modified Colligan with Crumly. So that the image that is being sent to a computer that is restoring its hard to like new would be able to have used the

digital signature of the image to so that the user can verify that the digital image has not been altered.

Claim Rejections - 35 USC § 103

Claims 1-5 and 15-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Colligan et al (U.S. 6,519,762) in view of Crumly (U.S. 20030161475).

Colligan teaches with respect to claim 1, a method for preparing an authenticable and verifiable image of a module, the method comprising: receiving a module image (see Colligan column 9 lines 34-38); adding to the module image a size and location block (see Colligan column 9 lines 34-38).

Colligan does not teach adding to the module image an authentication block including a cryptographically protected module-specific public key and a clear-text version of the module-specific public key to produce an authenticable image; and adding to the authenticable image a verification block that includes a digital signature prepared from the module image.

Crumly teaches adding to the module image an authentication block including a cryptographically protected module-specific public key (see Crumly paragraph 0025) and a clear-text version of the module-specific public key to produce an authenticable image (see Crumly paragraph 0025 and 0036); and adding to the authenticable image a verification block that includes a digital signature prepared from the module image (see Crumly paragraph 0036). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have included a digital signature of the image to so that the user can verify that the

digital image has not been altered. Therefore one would have been motivated to have included a digital signature of the image (see Crumly paragraph 0036).

With respect to claim 2, wherein adding to the module image a size and location block further includes: adding, in a specific location, a header that includes an image size, location, and globally unique identifier, that describes a size and location of the firmware image within a flash memory or other non-volatile memory, and that identifies a class of machines for which the firmware module has been created (see Colligan column 9 lines 12-38).

With respect to claim 3, wherein adding to the module image an authentication block including a cryptographically protected module-specific public key and a clear-text version of the module-specific public key to produce an authenticable image further includes: adding to the module image an authentication block including an encrypted, hashed module-specific public key and a clear-text version of the module-specific public key to produce an authenticable image (see Crumly paragraph 0025).

With respect to claim 4, wherein adding to the authenticable image a verification block that includes a digital signature prepared from the module image further includes: adding to the authenticable image a verification block that includes a digital signature prepared by hashing the module image and encrypting the hashed module image with a module-specific private key (see Crumly paragraph 0036).

With respect to claim 5, a computer instructions that together compose a program that carries out the method of claim 1 stored in computer readable medium (see Colligan column 9 lines 34-38).

With respect to claim 15, an authenticable and verifiable image of an a module stored in a computer-readable medium comprising: a module image, including a size, location, and globally unique-identifier block (see Colligan column 9 lines 34-38); an authentication block (see Crumly paragraph 0025 and 0036); and a verification block (see Crumly paragraph 0036).

With respect to claim 16, wherein the authentication block contains an encrypted, hashed module-specific public key and a clear-text version of the module-specific public key to produce an authenticable image (see Crumly paragraph 0025 and 0036).

With respect to claim 17, wherein the verification block that includes a digital signature prepared by hashing the module image and encrypting the hashed module image with a module-specific private key (see Crumly paragraph 0036).

With respect to claim 18, a method for preparing an authenticable and verifiable image of a module, the method comprising: a module-image receiving step (see Colligan column 9 lines 34-38); a size-and-location-data adding step that adds size-and-location data to the received module image (see Colligan column 9 lines 34-38); an authentication-adding step that adds, to the module image, authentication information including a cryptographically protected module-specific public key and a clear-text version of the module-specific public key (see Crumly paragraph 0025 and 0036); and a verification-block-adding step that adds a digital signature prepared from the module image to the module image (see Crumly paragraph 0036).

Conclusion

This application contains claims 6-14 drawn to an invention nonelected with traverse in the reply filed on 10/29/2007. A complete reply to the final rejection must include cancellation of nonelected claims or other appropriate action (37 CFR 1.144) See MPEP § 821.01.

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Devin Almeida whose telephone number is 571-270-1018. The examiner can normally be reached on Monday-Thursday from 7:30 A.M. to 5:00 P.M. The examiner can also be reached on alternate Fridays from 7:30 A.M. to 4:00 P.M. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

/Devin Almeida/
Examiner, Art Unit 2132
7/9/2008

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2132